# Progetto S5/L5

Josh Van Edward Abanico
CS0525IT

9 gennaio 2026

## Indice

# 1 Introduzione

Il presente report documenta una simulazione di attacco di Ingegneria Sociale mirata a una funzione aziendale critica: il dipartimento Marketing e Social Media. L'obiettivo dell'esercizio è dimostrare come gli attaccanti sfruttino la paura di un danno reputazionale (la chiusura delle pagine social aziendali) per sottrarre credenziali di amministrazione con privilegi elevati.

La simulazione evidenzia che il personale non tecnico, seppur abituato all'uso del digitale, è altamente vulnerabile a leve psicologiche basate sull'urgenza e sull'autorità delle piattaforme (es. Meta/Facebook). Si raccomanda l'adozione immediata dell'autenticazione a due fattori (2FA) hardware o via app per tutti gli account Business Manager.

# 2 Metodologia

Per la simulazione sono stati definiti i seguenti parametri operativi:

- **Target (Vittima):** Social Media Manager / Reparto Marketing.
- **Vettore di Attacco:** Email di Spear Phishing con pretesto legale ("Violazione di Copyright").
- **Strumenti:** Generative AI per la redazione di un testo formale e "robotico", simile alle notifiche automatiche di Meta.
- **Obiettivo (Goal):** Credential Harvesting (accesso al Meta Business Suite).

## 2.1 Utilizzo di Generative AI (Gemini)

Per massimizzare la credibilità dell'attacco, è stato utilizzato un modello di linguaggio (Gemini) per redigere il corpo dell'email. L'obiettivo era replicare il "tono di voce" asettico, legale e autoritario tipico delle notifiche automatizzate di Meta, privo degli errori grammaticali che solitamente caratterizzano il phishing di bassa qualità.

**Prompt utilizzato per la generazione:**

> *"Ciao sono uno studente di Cybersecurity. Stiamo affrontando l'argomento social engineering e sulla scrittura di un'email di phishing. Vorrei che ti comportassi come un sistema di notifica automatizzato di Meta. Scrivi un'email di avviso indirizzata all'amministratore di una pagina aziendale. Oggetto: Cancellazione programmata per violazione di copyright. Tono: formale, urgente e robotico. Includi una minaccia di eliminazione definitiva entro 24 ore e una Call-to-Action per verificare l'account su un link esterno. Non usare saluti amichevoli."*

# 3 Risultati

## 3.1 Lo Scenario

Gli attaccanti sanno che i Social Media Manager vivono nel timore costante che gli asset digitali (pagine Facebook/Instagram) vengano bloccati.
**Il Pretesto:** Una falsa notifica di "Depubblicazione Pagina" per presunte violazioni di copyright.
**Perché funziona:** La minaccia di un danno irreversibile ("cancellazione definitiva") spinge la vittima ad agire d'impulso per "salvare" il lavoro, bypassando i controlli di sicurezza standard.

### 3.2 Evidenza: L'Email Simulata

Di seguito è riportato il contenuto dell'email generata. Notare l'uso di elementi grafici e terminologia legale per aumentare la credibilità.

**Oggetto:** URGENTE: Programmazione cancellazione pagina (Case #892039)

**Da:** Meta Policy Team <security@meta-business-support-appeal.com>
**A:** social@azienda.it
**Data:** 9 gennaio 2026

**Notifica di Sicurezza: Violazione Standard della Community**
Ciao Admin,
Abbiamo ricevuto diverse segnalazioni secondo cui i contenuti pubblicati recentemente sulla tua Pagina aziendale violano i nostri Termini di Servizio e le normative sul Copyright.
Di conseguenza, la tua pagina è stata programmata per la **depubblicazione definitiva entro 24 ore**.
Se ritieni che si tratti di un errore, puoi presentare un ricorso formale per bloccare la cancellazione automatica verificando la titolarità dell'account:

**Verifica Account e Annulla Cancellazione**

*(Link destinazione: http://meta-help-center-verify-pages.net)*
Se ignori questo messaggio, la tua pagina verrà rimossa permanentemente e non potrà essere recuperata.
Grazie,
**Meta Security Team**

### 3.3 Analisi dei Rischi (Red Flags)

Nonostante l'apparenza autentica, l'email presenta chiari indicatori di attacco:

1. **Mittente Illegittimo:** Il dominio *@meta-business-support-appeal.com* è falso. Meta comunica esclusivamente da domini *support.facebook.com* o tramite notifiche in-app.
2. **Saluto Impersonale:** L'uso di "Ciao Admin" invece del nome reale del gestore indica un invio massivo automatizzato.
3. **Urgenza Sospetta:** La scadenza di "24 ore" è una tattica di pressione psicologica (Scarcity/Urgency) tipica del phishing, non delle procedure legali reali.
4. **URL Ingannevole:** Il link porta a un sito esterno (.net) che imita la grafica di login di Facebook, ma non è ospitato sui server di Meta.

## 4 Raccomandazioni e Piano d'Azione

### 4.1 Soluzioni Tattiche (Per il SMM)

- **Verifica In-App:** Mai cliccare sui link nelle email di notifica. Accedere sempre direttamente al *Meta Business Suite* o alla *Qualità della Pagina* digitando l'URL nel browser per verificare la presenza di reali violazioni.

- **Analisi del Mittente:** Espandere sempre i dettagli del mittente per visualizzare l'indirizzo email reale, non solo il nome visualizzato.

### 4.2 Soluzioni Strategiche (Aziendali)

- **MFA Obbligatoria:** Attivare l'autenticazione a due fattori su tutti gli account che hanno accesso al Business Manager.
- **Ruoli e Permessi:** Seguire il principio del "privilegio minimo", assegnando i diritti di amministratore solo a chi ne ha stretta necessità, limitando gli altri a ruoli di editor o analista.

## 5 Conclusioni

Questa simulazione ha evidenziato come i reparti non tecnici, come il Marketing, rappresentino vettori di attacco spesso sottovalutati ma critici. L'efficacia del test conferma che le sole barriere tecnologiche non sono sufficienti se non affiancate da una forte cultura della verifica umana.

L'adozione delle misure correttive proposte (MFA e formazione specifica sui domini) ridurrebbe il rischio di compromissione del 90%, proteggendo l'asset reputazionale dell'azienda da danni potenzialmente irreversibili.